



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,699	03/27/2001	Doug L. Rollins	MTIPAT.187A	9926
20995 7590 01/25/2008 KNOBBE MARTENS OLSON & BEAR LLP 2040 MAIN STREET FOURTEENTH FLOOR IRVINE, CA 92614			EXAMINER NGUYEN, MINH DIEU T	
			ART UNIT 2137	PAPER NUMBER
			NOTIFICATION DATE 01/25/2008	DELIVERY MODE ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcarter@kmob.com  
eOAPilot@kmob.com

## Office Action Summary

Application No.

09/818,699

Applicant(s)

ROLLINS, DOUG L.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 07 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1, 5, 7, 8, 12-14, 17 and 20-24 is/are pending in the application.
- 4a) Of the above claim(s) 2-4, 6, 9-11, 15, 16, 18 and 19 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 5, 7, 8, 12-14, 17 and 20-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 11/28/07.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the communication dated 11/7/07 with the amendments to claims 1, 5, 8 and 12, the cancellation of claims 2-4, 6, 9-11, 15-16 and 18-19 and the addition of claims 21-24.
2. Claims 1, 5, 7-8, 12-14, 17 and 20-24 are pending.

### ***Information Disclosure Statement***

3. The information disclosure statement filed 11/28/07 has been placed in the application file and the information referred to therein has been considered as to the merits.

### ***Response to Arguments***

4. Applicant's arguments filed 11/7/07 have been fully considered but they are not persuasive. The Applicant argues that Hanna teaches away from the claims invention by including decryption key information with encrypted data. The Examiner respectfully disagrees. Hanna discloses the encrypted first decryption key along with the encrypted data are sent to the client, where the first decryption key is encrypted with the public key of client (Hanna: col. 5, lines 21-24), the decryption key is not sent in the clear, the transmitted encrypted decryption key is gibberish, unintelligible data to unauthorized parties, as such it is without data indicative of an associated decryption key. Further as to the claim containing a negative limitation (i.e. without data indicative of an associated

decryption key), a lack of literal basis in the specification for a negative limitation may not be sufficient to establish a prima facie case for lack of descriptive support. Ex parte Parks, 30 USPQ2nd 1234, 1236 (Bd. Pat. App. & Inter. 1993). The mere absence of a positive recitation is not basis for an exclusion (MPEP 2173.05 (i)).

On the same argument, the Applicant submits Pond discloses much of the data necessary to decrypt an encrypted file is attached permanently to the file. On the same line of response, the Examiner disagrees, even when at least one of the key stream flags of the key mix must be set, the key mix itself is not enough to decrypt the information because the key mix is utilized to designate which keys, in addition to the Mandatory Key, are to be used for encryption and decryption of the protected file (Pond: col. 3, lines 45-48), further the key mix is encrypted using the mandatory key (as submitted by the applicant, Pond: col. 4, lines 17-19) (i.e. encrypted information only yields gibberish, unintelligible data to unauthorized parties, as such it is without data indicative of an associated decryption key).

The Applicant argues that Eldridge fails to disclose other limitations of the base claims. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

***Specification***

5. The amendment filed 11/7/2007 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "if the requested data is encrypted with the encryption key, sending the encrypted data to the client computer system **without data indicative of an associated decryption key**" and "if the requested data is unencrypted,..., sending the encrypted data to the client computer system **without data indicative of an associated decryption key**".

Applicant is required to cancel the new matter in the reply to this Office Action.

***Claim Rejections - 35 USC § 112***

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1, 5 and 8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. There is no support for the amended limitation "if the requested data is encrypted with the encryption key, sending the encrypted data to the client computer system **without data indicative of an associated decryption**

**key"** and "if the requested data is unencrypted,..., sending the encrypted data to the client computer system **without data indicative of an associated decryption key**". At best, paragraph 0045 and Fig. 5 disclose method steps of transferring data over a computer network from a network server to a client computer system, however it is silent on the teaching of **without data indicative of an associated decryption key**.

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1, 5, 8, 12-13, 17, 20-22 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna et al. (7,178,021) in view of Pond et al. (4,864,616) in view of Simmons et al. (2001/0039659) and further in view of Fan et al. (6,310,692).

a) As to claims 1 and 8, Hanna discloses a method of transferring data over a computer network from a network server to a client computer system (Hanna: col. 1, lines 17-20), the method comprising: receiving a request by a requestor using a client computer system (Hanna; col. 5, lines 15-16) for data from at least one network server storing data, at least some of the data stored by the network server being encrypted (Hanna: col. 4, lines 16-21); if the requested data is encrypted with the encryption key, sending the encrypted data to the client computer system without data indicative of an associated decryption key (i.e. the encrypted first decryption key along with the

encrypted data are sent to the client, where the first decryption key is encrypted with the public key of client (Hanna: col. 5, lines 21-24), the decryption key is not sent in the clear, the transmitted encrypted decryption key is gibberish, unintelligible data to unauthorized parties, as such it is without data indicative of an associated decryption key).

Hanna is silent on the capability of checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key.

Pond is relied on for the teaching of checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key (i.e. the system checks to see if a banner is present, wherein a banner indicates if the file is protected, Pond: col. 3, lines 43-44; col. 8, lines 26-27).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key in the system of Hanna, as Pond teaches, so as to protect sensitive data files with proper labels (Pond: col. 1, lines 6-10).

The combination of Hanna and Pond is silent on the capability of if the requested data is unencrypted (see Pond), automatically retrieving the encryption key associated with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data; and sending the encrypted data to the client computer system without data indicative of the associated decryption key.

Simmons is relied on for the teaching of automatically retrieving the encryption key associated with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data; and sending the encrypted data to the client computer system without data indicative of the associated decryption key (Simmons: 0016, 0041, 0046).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of automatically retrieving the encryption key associated with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data; and sending the encrypted data to the client computer system without data indicative of the associated decryption key in the system of Hanna and Pond, as Simmons teaches, so as to securely protect transmitted data over a network.

The combination of Hanna, Pond and Simmons is silent on the capability of sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor.

Fan is relied on for the teaching sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor (i.e. notification is



generated and transmitted, Fan: col. 5, lines 45-49. It is obvious that what is in the notification is purely the design choice).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor in the system of Hanna, Pond and Simmons, as Fan teaches, so as to dynamically managing resources (Fan: col. 1, lines 8-12).

b) As to claim 5, the majority of this claim is in claim 1 with the addition of the following limitation: automatically generating independently of information from a network server a public encryption key and a corresponding private encryption key in a client computer system; storing the public encryption key and the corresponding private encryption key in the client computer system (Simmons: 0041). Pond discloses associating an attribute with a data file, the attribute indicating whether the data file is encrypted (Pond: col. 3, lines 43-44; col. 8, lines 26-27), and the attribute indicating an owner of the public encryption key (Hanna: col. 5, lines 4-6). Hanna discloses public and private encryption key where the data file is encrypted with public key (Hanna: col. 4, lines 53-57).

c) As to claims 12, 17 and 20, the combination of Hanna, Pond, Simmons and Fan discloses the method of claim 1, further comprising sending the requested data to the client computer system only if the requested data is encrypted and if the requestor is the owner of the encryption key (Hanna: col. 5, lines 19-25).

d) As to claims 13, 21-22 and 24, the combination of Hanna, Pond, Simmons and Fan discloses the method of claim 1, wherein the encryption key is derived at least in part from an identification code, identification code is uniquely associated with the client computer system, Pond: col. 5, lines 20-40).

10. Claims 7, 14 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna et al. (7,178,021) in view of Pond et al. (4,864,616) in view of Simmons et al. (2001/0039659) in view of Fan et al. (6,310,692) and further in view of Eldridge et al. (6,094,721).

The combination of Hanna, Pond, Simmons and Fan does not explicitly disclose the public and private keys are based on a password.

Eldridge discloses a method and apparatus for updating the password status of one of more servers in a client/server environment comprising public and corresponding private key derived from password (Eldridge: col. 5, lines 33-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of generating public and private key from a password as Eldridge teaches in the system of Hanna, Pond, Simmons and Fan so as to secure password authentication to access (Eldridge: col. 1, lines 15-17).

### ***Conclusion***

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you

Application/Control Number:  
09/818,699  
Art Unit: 2137

Page 11

have questions on access to the Private PAIR system, contact the Electronic Business  
Center (EBC) at 866-217-9197 (toll-free).



MinhDieu Nguyen  
Patent Examiner  
1/22/08